REMARKS

Claims 1-5, 10-14, 16-23 and 25 are currently active.

Claims 6-9, 15 and 24 have been canceled.

The Examiner has objected to the drawings. Amended drawings are included herewith, with the amendments shown in red. It is submitted these changes to the drawings will obviate the objection. Formal drawings will be provided when the application is allowed.

The Examiner has rejected Claims 1, 2, 14-15 and 22-23 as being anticipated by Dacier. Applicants have amended the claims so the limitations of Claim 3 are found in Claim 1, the limitations of Claim 16 are found in Claim 14 and the limitations of Claim 24 are found in Claim 22. Claims 3, 16 and 24 were not rejected because of anticipation reasons with respect to Dacier.

The Examiner has rejected Claims 3-13, 16-21and 24-25 as being unpatentable over Dacier in view of Reichmeyer. Applicants respectfully traverse this rejection. As noted above, Claim 3 is now written in independent form as Claim 1, with all the limitations of its base claim and any intervening claims. This is also the case in regard to Claims 16 and 24, and Claims 14 and 22, respectfully.

Referring to Dacier, there is disclosed a communications network for preventing third party intrusions attempting to divert information being communicated on the network between parties. Dacier teaches that each switch maintains a database of the network's topology. To reduce the information each switch has to maintain in its database about the topology of the network, the PNNI standard provides that the network can be logically defined as a hierarchy with nodes on each level of the hierarchy arranged in peer groups. Under PNNI, the switches exchange information with one another on a regular basis to inform every switch about changes in the topology of the network. Information exchange is performed using a process called flooding. Flooding involves a hop-by-hop propagation of topology information in packets to all the switches in a peer group and two adjoining switches of the peer groups. See column 1, lines 25-46. It should be noted, that Dacier teaches a standard prior art system that applicants described in the background of the invention of the above-identified patent application. It should be further noted, that the problem that applicants identified that exists in the prior art was that configuration information was not provided from a single location. Applicants' claimed invention has been amended to more specifically describe that not only is configuration information made part of the topology data base, but what type of configuration information is also made part of the topology database.

Dacier teaches the network 18 passes information from one end system 10 to another end system 12 through intervening switching nodes 14 and physical links 16 in accordance with the PNNI standard. To reduce the amount of information that must be stored

in the database of each network switch, the network 18 is addressed as a hierarchy of nodes arranged in peer groups. See column 3, lines 3-10. Dacier teaches that each node advertises a set of reachabilities. A reachability is basically a prefix used to match the destination address for a call setup, the prefix length bit and prefix itself. The process to select the destination switch first has the calling switch receiving a call setup message that contains the address of the destination device. The switch selects among the reachabilities in this topology database the one featuring the longest prefix matching the destination address. If that route is available, the call is routed to the switch advertising the selected reachability. If that route is not available, another route is selected. If no route is available, an appropriate message is passed to the signaling end system 10. See column 3, lines 40-55.

Dacier teaches that a malicious user could configure a switch so that it always advertises longest prefixes to be the destination of the calls it is interested in. See column 3, lines 58 and 59. Once the traffic is rerouted, it is possible to make sure that all communicated information reaches its intended destination through an alternate path. The attack is completely transparent for the sender 10 and intended receiver 12 of the routing packets. See column 4, lines 37-40.

Dacier states that it teaches a technique that will automatically detect the existence of all overlapping reachabilities. Since not all reachabilities that overlap are suspicious or problematic, the only ones that are suspicious are those that are not consistent

with what is considered as normal. In addition, to malicious overlapping reachabilities, errors are caused by accidental overlapping reachabilities. The technique taught by Dacier operates on both malicious and accidental overlapping reachabilities. See column 4, lines 42-57.

Dacier teaches that to distinguish between suspicious and non-suspicious reachabilities, a model of the previous behavior of the network is built from the topology database stored in each of the switches of a peer group. Whenever a new reachability is announced by a switch, a check of the reachability is made in real time to see if it is consistent with what had been observed in the past. An inconsistent change is seen as suspicious and treated as such. Dacier teaches that since all switches of the peer group contain the same data in the topology database, you only need one switch implementing an algorithm that Dacier describes detect intrusions taking place at any place in its peer group. See column for, line 66 deaths column 5, line three. As is clear from this description, Dacier does not teach or suggest anything about including configuration information in a topology data base. The focus of Dacier involves overlapping reachabilities. Again, Dacier has defined reachability as basically a prefix used to match the destination address for a call setup, the prefix length bit and prefix itself. See column 3, lines 39-41. The issue of malicious or accidental overlapping reachabilities that Dacier is concerned about is totally distinct and has nothing to all to do with applicants claimed invention, which is to have a database having configuration information that includes the name of the switch, an IP address of the switch, a software version of the switch, or a hardware type of the switch.

The specific types of configuration information, is just that, and is not representative of some form of some type of information, as the examiner suggests. For instance, in regard to Claim 6, the Examiner states that Dacier teaches the name of the switch because the name of the switch comprises a peer address and a unique number. The peer address, is exactly that, the peer address, and is not the name of the switch. The unique number, is just that, the unique number, not the name of the switch. The name of the switch is only the name of the switch. The peer address and unique number are not configuration information and by the presence of both, does not suddenly make configuration information. Accordingly, Dacier does not teach or suggest a topology data base having configuration information as found in amended Claim 1.

Referring to Reichmeyer, there is disclosed a method and apparatus for remotely configuring a network device. Reichmeyer teaches that as networks continue to become more complex, the simplification of the configuration process is becoming increasingly attractive and necessary. Reichmeyer teaches that the parameters controlling behavior of a network and device are typically stored within a configuration file. The configuration file may be created by the networking device itself or by some other configuration-capable device and then installed on the network device. See column 2, lines 45-49.

Reichmeyer teaches that the simple network management protocol (SNMP), may be utilized to transfer configuration information from a remote location to a network device. See column 4, lines 44-48. Reichmeyer teaches the network 22 includes a central management system 24 that includes a central configuration server 26 coupled to a topology database 28. The topology database 28 is utilized by the central management system 24 to store and retrieve information concerning the physical and logical topology of the network 22. The physical topology information includes descriptions of physical network devices, and the physical connectivity. For example, information concerning a device type (for example, router or switch), level 2 addresses and orts may be included within the physical topology information. The logical topology information includes level 3 interface information and includes a network address, subnet and routing protocol information. The physical topology information can be constructed in closing a number of different mechanisms. See column 4, lines 51-66.

Again, just as with respect to Dacier, there is no teaching or suggestion of a topology data base having configuration information where the configuration formation includes the name of the switch, the IP address of the switch, the software version of the switch and the hardware type of the switch, as found in amended Claim 1. This follows because Reichmeyer is concerned with being able to remotely configure a network device and not to disseminate configuration information as described above, which has been traditionally understood to be outside what has been included as part of the topology database. Simply

speaking, the applied art of record is missing this claim limitation. For this reason alone, amended Claim 1 is patentable over the applied art record.

Furthermore, there is no teaching or suggestion in the references themselves to combine what the Examiner purports to be the relevant teachings in the references to arrive at applicants' claimed invention. Patent law requires such a teaching or suggestion.

The only reason to combine these references is from the hindsight of applicants' own claims, which is again contrary to patent law. The Examiner is using the elements of applicants' claimed invention as a road map to find the various elements in different references, and having found them, concludes that applicants' claimed invention is obvious. However, besides having to use hindsight, which is contrary to patent law, the Examiner is also ignoring the context in which the teachings are found in the references, which is also contrary to patent law. Dacier has the context which is concerned with malicious or accidental overlapping of reliabilities. Reichmeyer has the context which is concerned with remotely configuring a network device. These two contexts are completely distinct and have no relationship. No one skilled in the art would look to one reference from the other to arrive at applicants' claimed invention. Specifically, there is no reason why Dacier will have any need or use whatsoever of an SNMP query. To have such a need or use, let alone to be able to be combined with Reichmeyer, would require Dacier to somehow or other be completely redesigned so that it focuses on a totally different purpose, and ignores its concern regarding

malicious or accidental overlap in reliabilities. This shows that applicants' claimed invention is not obvious, because it would require significant amount of research and development and design work to modify the applied art of record to arrive at applicants' claimed invention. Accordingly, for these additional reasons, Claim 1 is patentable.

Claims 4, 5 and 10-13 are dependent to parent Claim 1 and are patentable for the reasons Claim 1 is patentable.

Claim 14 is patentable for the reasons Claim 1 is patentable. Claims 17-21 are dependent to parent Claim 14 and are patentable for the reasons Claim 14 is patentable.

Claim 22 is patentable for the reasons Claim 1 is patentable. Claims 23 and 25 are dependent to parent Claim 22 and are patentable for the reasons Claim 22 is patentable.

In view of the foregoing amendments and remarks, it is respectfully requested that the outstanding rejections and objections to this application be reconsidered and withdrawn, and Claims 1-5, 10-14, 16-23 and 25, now in this application be allowed.

CERTIFICATE OF MAILING

I hereby certify that the correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on 3/13/03

Ansel M. Schwartz
Registration No. 30, 587
3/13/03
Date

Respectfully submitted,

SIVARAMAKRISHNA KUDITIPUDI, ET AL.

By Ansel Schwartz

Ansel M. Schwartz, Esquire
Reg. No. 30,587
One Sterling Plaza
201 N. Craig Street
Suite 304
Pittsburgh, PA 15213
(412) 621-9222

Attorney for Applicant

Version with markings to show changes made to the claims

1. A switch of a network comprising:

a topology database having configuration information, the configuration information includes a name of the switch, an IP address of the switch, a software version of the switch, and hardware type of the switch; and

a mechanism for sending the configuration information from the topology database to the network and for receiving configuration information from the network and storing it in the topology database, the sending and receiving mechanism include a switch agent for receiving configuration information from the network, the switch agent looks up in the topology database and returns requested information of an SNMP query from the network.

4. A switch as described in Claim [3] 1 wherein the switch agent forms an SNMP query to the network.

10. A switch as described in Claim [9] 5 wherein the configuration information includes a unique ID of the switch.

14. A telecommunications system comprising:

S switches, where S is an integer greater than or equal to 2, each switch having a topology database with all configuration information of the S switches, any one switch providing all the configuration information for all of the S switches, the configuration information includes a name of the switch, an IP address of the switch, a software version of the switch, and hardware type of the switch, the switches send configuration information to each other, the switches send SNMP queries to each other to return retrieved configuration information from each other, and the switches respond to the SNMP queries by sending the requested configuration information to the other switches which sent the SNMP queries.

17. A system as described in Claim [16] 14 wherein the switches attach a systems information group to a nodal information group to propagate the configuration information to the other switches in response to an SNMP query.

22. A method for operating a telecommunications network comprising the steps of:

placing configuration information of a first switch of the network into a topology database of the first switch, the configuration information includes a name of the switch, an IP address of the switch, a software version of the switch, and hardware type of the switch; [and]

sending an SNMP query from the second switch to the first switch for configuration information in the topology data base of the first switch; and

propagating the configuration information of the first switch to a second switch of the network.

25. A method as described in Claim [24] 23 wherein the propagating step includes the steps of attaching a system information group having the configuration information from the topology data base of the first switch requested by the SNMP query to a nodal information group; and propagating the system information group attached to the nodal information group to the second switch.

OIPE
MAR 1 8 2003
PATENT & TRADEMARK OFFICE

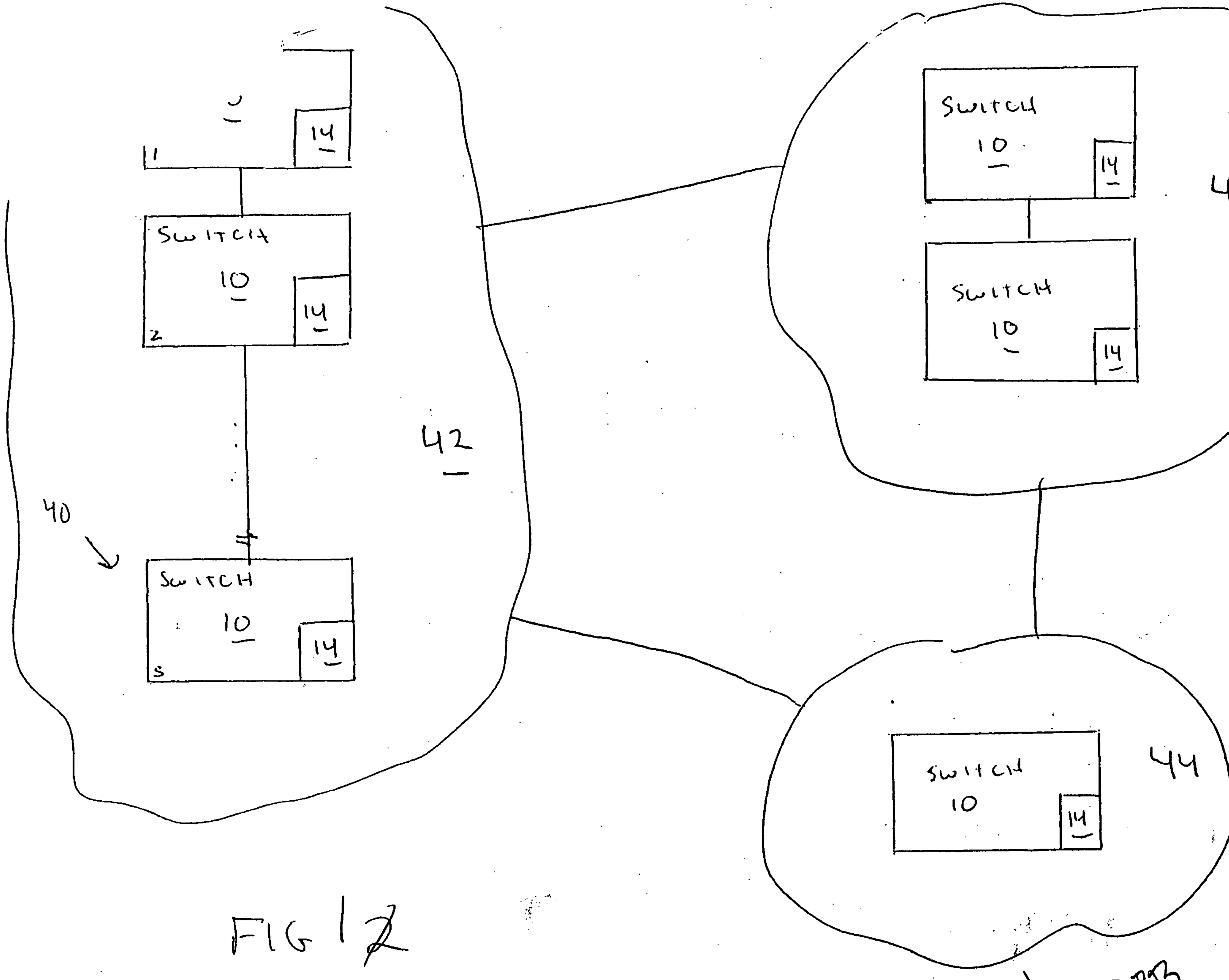

FIG 1~~2~~

Approved, DBB

#6

OIPE JC14
MAR 10 2003
PATENT & TRADEMARK OFFICE

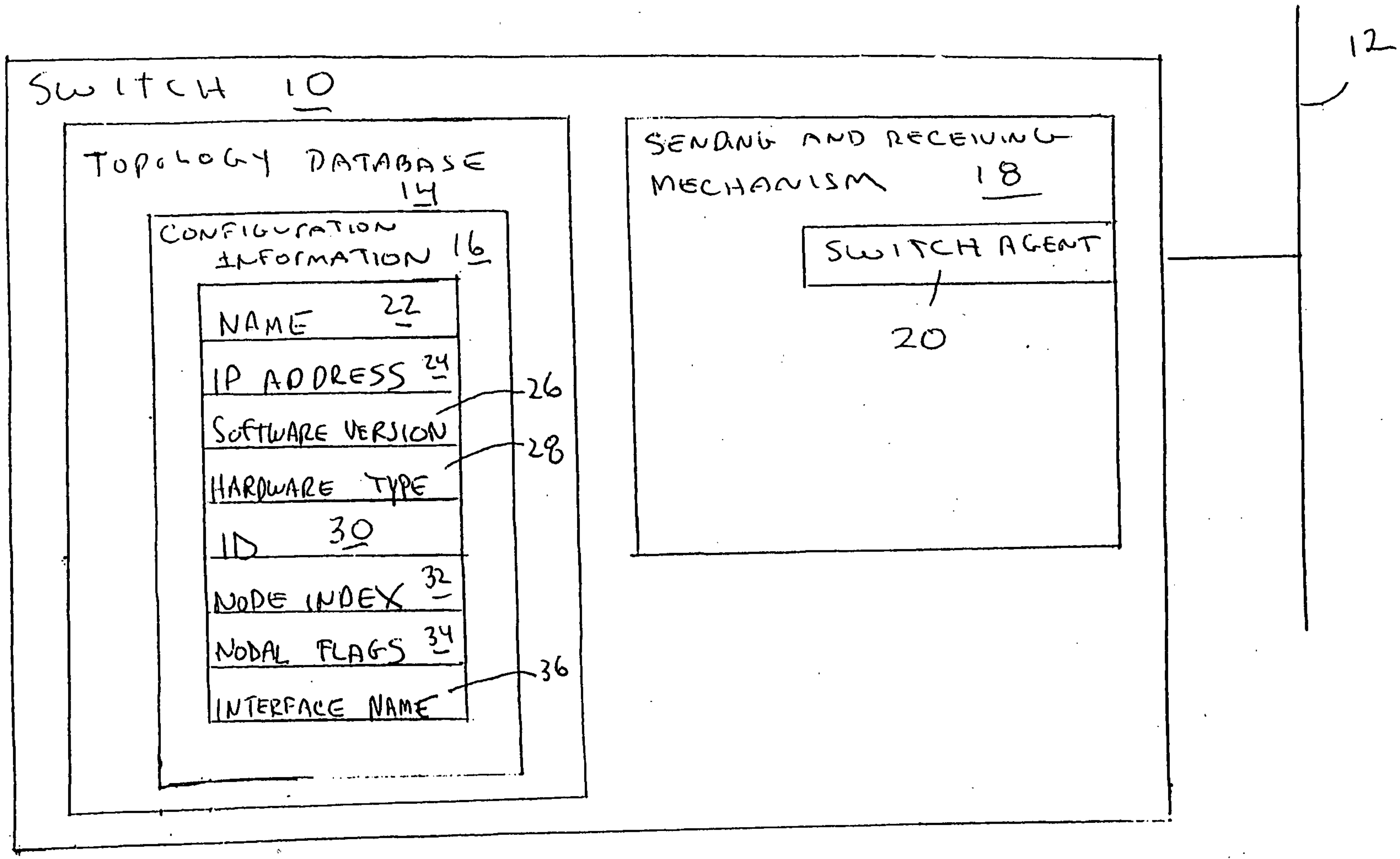

FIG ~~1~~ 2